



CVE-2017-5227

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-5227
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-23 16:59:00 UTC
Updated	2017-08-16 01:29:00 UTC
Description	QNAP QTS before 4.2.4 Build 20170313 allows local users to obtain sensitive Domain Administrator password information

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Qnap	Qts	All	All	All	All

References

Reference
QNAP QTS CVE-2017-5227 Local Information Disclosure Vulnerability
QNAP QTS < 4.2.4 - Domain Privilege Escalation - Hardware local Exploit
Security Vulnerabilities Addressed in QTS 4.2.4 Build 20170313
QNAP, Inc. - Network Attached Storage (NAS)
QNAP QTAP Qualcomm components Multiple Unspecified Security Vulnerabilities
QNAP Storage Devices Multiple Flaws Let Remote Users Inject SQL Commands, Steal Cookies, Conduct Cross-Site Scripting and Clickjacking
www.ush.it/team/ush/hack-qnap/qnap.txt
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)